

AIR WAR COLLEGE

AIR UNIVERSITY

UNITED STATES PREPAREDNESS TO RESPOND TO A
“MUMBAI-STYLE” ATTACK WITHIN THE HOMELAND

by

Brad C. Felling, Lt Col, USAFR

A Research Report Submitted to the Faculty
In Partial Fulfillment of the Graduation Requirements

17 February 2010

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Certificate.....	i
Contents.....	ii
Illustrations.....	iii
Biographies.....	iv
Introduction.....	1
Mumbai Attack Overview.....	2
United States vs. India Counter-options.....	4
United States Preparedness Plans & Exercises.....	7
Potential Gaps in United States Preparedness.....	10
Federal Authority Gap.....	10
10 U.S. § Code 380 Section 1033.....	11
State and Local Authority Gap.....	15
Foreign Intelligence Surveillance Act.....	16
4th Amendment to the Constitution.....	17
Information Sharing Success Stories.....	18
Conclusion.....	20
Bibliography.....	22
Endnotes.....	23

Illustrations

Page

Figure 1. Federal Intelligence Surveillance Act Minimization Procedures.....	18
--	----

Biographies

LtCol Brad C. Felling United States Air Force Reserve

Lieutenant Colonel Felling is a student attending Air War College (in-residence), Maxwell AFB. Prior to his current assignment, he served as the NORAD/USNORTHCOM Operations Liaison Officer at The National Counterterrorism Center (NCTC), McLean Virginia. He also served as Individual Mobilization Augmentee (IMA) to the Chief, CSAR and Special Activities Division for the Headquarters, Air Force Directorate of Current Operations and Training. Previously, he was IMA to the Chief, Reserve Operations Requirements Division for Headquarters, Air Force Reserve. He was commissioned in 1991 via the Reserve Officer Training Corps, graduating from The Catholic University of America, Washington D.C. During his career, he has served in positions at the Squadron, Group, and Wing levels including Squadron Flight Commander, Squadron and Group Executive Officer, Chief of Wing Contingency Plans, and Chief of Wing Public Affairs. Additionally, he was the Air Force Special Operations Command Liaison Officer to the United States Army Special Operations Command Combat Applications Group (Airborne). Lieutenant Colonel Felling's combat support experience includes Airborne Counter-Drug Operations in South America and Republic of Korea Airborne Surveillance Operations. His combat experience includes three tours of duty in Afghanistan supporting Operation Enduring Freedom and three tours of duty in Iraq supporting Operation Iraqi Freedom. He is a Basic Parachutist, with 27 static line jumps from C/MC-130, CASA-212, and C-141 aircraft. He has also earned The Federal Republic of Germany parachutist wings. He is a Senior Navigator with over 1,800 flight hours in E-3B/C AWACS and AC-130U Gunships.

Brad C. Felling Assistant to the Special Agent in Charge, Federal Air Marshal Service Washington Field Office

Mr. Felling was hired by the Federal Air Marshal Service in May 2002. He occupied a critically-manned career field, Special Operations Navigator, in the U.S. Air Force, therefore, did not join the FAM Service until March 2004. Assigned to the Washington Field Office, Mr. Felling was formerly in charge of Squad 13, responsible for daily administration & evaluation of thirty Federal Air Marshals. He periodically served as DCA-Reagan Washington National Airport and IAD-Dulles International Airport Duty ATSAC, responding to aviation security situations and supporting transiting FAMS. He also periodically served as International FAM Team Liaison ATSAC at IAD Dulles International Airport, monitoring in/out processing of Austrian, Canadian, Dutch, German, and Japanese Air Marshals as they transit U.S. Customs.

Prior to joining the Federal Air Marshal Service, Mr. Felling served in the United States Air Force for over 12 years. He was an instructor navigator on AWACS and AC-130U gunships. His final active-duty position was Air Force Liaison Officer assigned to 1st Special Forces Operations Detachment –Airborne, at Ft. Bragg, North Carolina from 2001-2004. He has made three combat deployments to Afghanistan and three to Iraq. He is currently a Lieutenant Colonel in the U.S. Air Force Reserve on military leave from the FAM Service, attending U.S. Air Force Air War College, Maxwell Air Force Base, Alabama. Prior to his current student status, he was activated as the NORAD/USNORTHCOM Operations Liaison Officer at The National Counterterrorism Center (NCTC) in McLean, Virginia.

During his career with the Federal Air Marshal Service, he has served as Assistant Operations Officer at the Washington Field Office from 2004 to 2005, then again in 2007. He deployed to Louis-Armstrong International Airport following Hurricane Katrina to secure the airport and assist thousands of evacuees fly to relief centers. He was a member of a HQ FAMS inspection team assigned to examine transportation security at Chennai-Madras International Airport, in India, setting up diplomatic procedures and establishing security protocols for subsequent FAM missions to India. He represented OLE-FAMS HQ during man-made crises and natural disasters at the Federal Emergency Management Agency (FEMA) in Washington D.C.

Mr. Felling holds a Bachelor of Arts degree in English Literature from The Catholic University of America, Washington D.C. He holds a Masters of Science degree in Human Resource Development from The University of Oklahoma. He is a graduate of the Transportation Security Administration Leadership Development Program.

Introduction

American homeland defenders are quick to criticize the Government of India's (GoI) counterterrorism techniques, or lack thereof, in response to the attacks in Mumbai last November. But there are two major gaps in the areas of 1) Federal authority and 2) State and Local authority if the "whole of U.S. Government" was required to counter a "Mumbai-style" assault in the United States. This study will outline the Mumbai attacks, examine a homeland defense simulation mandated by the National Security Council (NSC) to amplify these gaps, and recount recent success stories demonstrating what departments and agencies are doing to remedy these two deficiencies.

On November 26, 2008, ten well-trained Lashkar-e-Taiba (LeT or "Army of the Pure") militants attacked seven targets and successfully detonated two IEDs in Mumbai, India. More than sixty hours later, when the GoI neutralized the last terrorist, 166 people, including 6 Americans, had been killed, and 308 had been injured.¹ Last year alone, there were reports of three "Mumbai-style" attacks: the February assault on the Kabul, Afghanistan government buildings, the March attack on the Sri Lankan Cricket Team, and the attack on the Manawan Police Academy, both in Lahore, Pakistan.²

How could such a devastating attack occur in a world-renowned city like Mumbai, the "Entertainment Epicenter" of India? Excerpts from a popular tour guide describe Mumbai, formerly known as Bombay, like this: "Measure out: one part Hollywood; six parts traffic; a bunch of rich power-moguls; stir in half a dozen colonial relics...add a smattering of swish bars and restaurants...equal parts of mayhem and order; as many bazaars as you have lying around...throw it all in a blender on high...and presto: Mumbai."³ Mumbai is also a port-city, with a major financial center. These characteristics can be applied to many burgeoning

metropolises in the United States. But considering that Mumbai is also home to vital Indian nuclear establishments and the Western Naval Command,⁴ one can see the potential for worldwide consequences on a much greater strategic scale, regardless of the attacked city or country.

Mumbai Attack Overview

Before proceeding further, the tactics, techniques and procedures used by LeT during the Mumbai attack should be identified.

- a. Pre-Operational Reconnaissance: Up to two years prior to the Mumbai attacks, LeT operatives were making sketches of potential targets and stockpiling weapons and IED-making equipment in Mumbai.
- b. Commando assault by well-trained operatives: The sole LeT survivor, Ajmal Amir Kasab, told Indian authorities he had been preparing for the Mumbai attack for one year. His training focused on small arms tactics, marine assault, and close-quarters battle. He was also issued 10 false identifications.⁵
- c. Soft, iconic targets: The 10 terrorists split into four teams, placed up to five IEDS around the city, and synchronized their conventional-style assaults on pre-identified targets. They also knew their targets, hit simultaneously, would inhibit a properly coordinated response by Indian authorities. The targets were also picked due to their landmark status, ensuring international media would immediately be on scene.⁶
- d. Maritime approach: The attackers used four different types of watercraft to travel from Karachi, Pakistan to the Sassoon Docks in Mumbai Harbor. They conducted a “brown-water”⁷ operation from inland Pakistan to Karachi, then trans-loaded to an awaiting Pakistani-flagged cargo ship in the Arabian Gulf. The attackers then hijacked an Indian-

flagged fishing vessel, killing all the crewmembers except the captain. After entering Mumbai harbor undetected, they killed the Captain, reprogrammed a GPS with exfiltration coordinates, then boarded two Rigid Hull Inflatable Boats (RHIBS) for their amphibious approach to the Sassoon Docks.

- e. Communications: The attackers used Voice Over Internet Provider (VOIP) technology, Blackberries, and fraudulently acquired sim cards to coordinate their attacks with each other and with their leadership in Pakistan. As the LeT leadership watched the Indian security response on television news broadcasts, they relayed this real-time intelligence to the attackers in Mumbai.⁸
- f. Simultaneous attacks to confuse responders: LeT employed armed assaults, car-jackings, drive-by shootings, prefabricated IEDs, targeted killings (policemen and selected foreigners), building takeovers, and barricade and hostage situations.⁹ The GoI thought they were under siege by a significantly larger force. The attackers opened fire in the emergency room of the hospital where ambulatory patients from the train station attack were being treated.
- g. Military-grade equipment: Each attacker was equipped with AK-56 (Chinese version of AK-47) automatic weapons, semi-automatic 9 mm. pistols, at least 300 spare rounds of ammunition, hand-grenades, and IED-making equipment.¹⁰
- h. IEDs: Each of the devices contained the high explosive RDX, ball bearings to create shrapnel, a digital timer, and a 9-volt battery.¹¹ Three failed to detonate, while two detonated via timing devices in cabs that were used to transport attackers to the train station and to the Taj Hotel.
- i. Social Media Exploitation: An estimated 80 messages, or "tweets," were sent to Twitter.com via SMS every five seconds, providing eyewitness accounts and updates. Some messages

were coming from hostages inside the hotels. The GoI sent a message asking tweeters to stop sending messages from Mumbai, worried that the terrorists were using the medium to gain information about what Indian security forces were doing.¹²

For 62 hours, ten terrorists brought a city of 20 million people to a standstill while the world watched. Now, one must consider the likelihood of a “Mumbai-style” attack occurring in the United States, especially after the U.S. Federal Bureau of Investigation (FBI) claims it is investigating threats of copycat attacks on U.S. interests.¹³

United States vs. India Counter-options

We assume that U.S. first responders are better trained and equipped than GoI police officers. But is there a baseline to gauge adequate preparedness in the homeland? Obviously, the attacks in Mumbai uncovered many weaknesses in GoI law enforcement, military, and political systems. But has the USG adequately internalized the potential consequences of this kind of attack?

While there has not been a parallel attack of this size and scope within the United States to compare response mechanisms and draw lessons-learned, there have been events in which heavily armed gunmen seriously challenged law enforcement agencies in urban environments similar to Mumbai. Two specific 1990’s shootouts that occurred in the two largest cities in California demonstrate that even well-trained and equipped law enforcement officers can be overmatched when engaged in paramilitary, urban combat situations.

On November 14, 1994, Victor Boutwell kept dozens of San Francisco Police officers at bay in the peaceful Pacific Heights section of the city for approximately 30 minutes before a SWAT officer shot him. Officer James Guelff, first at the scene, and armed with a department-issued six-shot revolver, was killed in action. Boutwell, dressed in camouflage, two layers of body

armor, and a bullet-resistant helmet, was armed with Belgian FB and Steyr automatic machine guns (both of which use M-16 compatible-ammunition), an automatic pistol, along with two other handguns, and 2,500 rounds of ammunition.¹⁴

On February 28, 1997, two heavily armed gunmen, protected by body armor impenetrable by most caliber handguns, engaged numerous Los Angeles Police Department officers in a gunfight that lasted for forty-five minutes outside a North Hollywood Bank. The shootout occurred not far from the Disney, Universal and Warner Bros. Studios, and the busy Hollywood Freeway was closed in both directions, tying up mid-day traffic.¹⁵ Stunned officers were out-gunned to such a degree they burst into a local gun store, and walked out with more powerful guns and ammunition. LAPD Police Commander Timothy McBride said "We have many suspects who have multiple guns, and they continue to out-gun us and fire at us at will."¹⁶

Nevertheless, a former CIA officer warned that Mumbai is the "worst-case active shooter problem" because it involved "multiple shooters, multiple locations, mobile threats, willingness to fight first responders and follow-on SWAT commando units, well equipped, and well-trained operatives, and a willingness to die."¹⁷ Like the L.A. and San Francisco law enforcement officers involved in the shootouts, the local Mumbai police were not equipped to confront heavily armed attackers. The first responders carried unserviceable revolvers, single bolt action rifles (British .305s developed in the World War II era), or bamboo sticks.¹⁸ Rather than shoot back at the attackers, most first responders ran away, hid behind civilians, were wounded, or killed.

Surprisingly, in early 2008, the GoI recognized these inadequacies and spent \$187 Million on "modernizing" local, state, and national law enforcement. But instead of properly equipping their police officers, they built new police stations and administrative offices, and purchased

luxury sedans for senior officers.¹⁹ To its credit, the GoI drafted a proposal to purchase AK-47 automatic assault weapons, but never followed up. The Indian National Security Guard (NSG), a loose equivalent to the FBI Hostage Rescue Team (HRT), was the only group that had bulletproof vests at the time of the attacks.

Mumbai police also lacked the sophisticated technical equipment used by the attackers, including night vision goggles, rifle scopes, and Global Positioning Systems. State and local communication devices were old and incompatible. BlackBerries, a staple among Mumbai civilians, could have been used to exchange tactical data and monitor new coverage, but were not issued to law enforcement officers. For instance, the military on-scene commander didn't comprehend the long term ramifications when he ordered power turned off at the scenes of attack.²⁰ One sharpshooter spent 60 hours stationed outside the Taj Majal Palace Hotel without firing a shot because he could not distinguish gunmen from civilian victims.²¹

Mumbai police had no equivalent to a SWAT team. After four hours of prolonged deliberations, the GoI made the decision that these were more than random acts of crime. They also decided to send the NSG to Mumbai. But the NSG is headquartered in the Indian capital of New Dehli, 875 miles from Mumbai. Further complicating the problem, NSG is not co-located with its Russian-contracted aircraft. Due to the transportation problems and protocols requiring a *written* request for assistance prior to the release of NSG assets and manpower, another five hours passed before the specially-trained NSG commandos arrived in Mumbai.²²

Once the GoI intervened in Mumbai and took overall control, it was clear that there was inadequate on-scene command at attack sites. Authorities cleared sections of buildings but failed to secure them, allowing the terrorists to reestablish positions.²³ A victim claimed security personnel let him pass unchecked as he escaped from one of the hotels. NSG forces failed to

identify themselves during the counter-attack. Victims didn't know if the NSG troops were terrorists or a rescue force.”²⁴

As mentioned earlier, the terrorists exploited media to their advantage. But the media may have directly interfered with response forces, as well. Militants gained information about police actions while watching news broadcasts. The media also played a telephone conversation with terrorists occupying the Nariman House and the Oberoi Hotel. Media spokesmen later defended their actions, claiming they helped law enforcement officials find the terrorists.²⁵

United States Preparedness Plans & Exercises

Pre-existing command and control procedures, better training and equipment, and increased interagency intelligence sharing should lessen the consequences of a “Mumbai-style” attack in the United States. But has the law enforcement community significantly updated their procedures since Mumbai? According to a 2009 report released by the National Tactical Officers Association (NTOA) “Law enforcement is unprepared to respond to even a single terrorist attack on a soft U.S. domestic target, such as a school. If attacks such as the Moscow Theatre Incident (2002) or the Beslan, School (North Ossetia, Russian Federation 2004) should occur here (U.S.) in the near future, the loss of the lives of hostages, other civilians who might become involved, and first responders could be calamitous”²⁶ Soft targets like these within the U.S. are also just as vulnerable as those attacked in Mumbai.

In December 2008, the NSC tasked the National Counterterrorism Center (NCTC) to evaluate how the U.S. would respond to a “Mumbai-style” attack.²⁷ The Protect and Defend the Homeland Division within the NCTC Directorate of Strategic Operational Planning convened an Interagency Working Group and coordinated a tabletop exercise simulating federal department and agency responses to an attack on a U.S. city, mirroring the events in Mumbai.

The U.S. city chosen as the scene of the simulated attacks needed to mirror Mumbai i.e. be a port city with access to the territorial waters of a neighboring country. The city had to be geographically separated from the seat of national power, similar to the distance between Mumbai and the Indian capital of New Delhi. The city also needed to be a transportation hub, an international tourist destination, and contain a major financial center and iconic landmarks.

Chicago was chosen as the simulated target city. The interagency participants received an intelligence bulletin warning of suspicious activity in the Chicago area, resembling the real-world intelligence report that the international intelligence community conveyed to the GoI in June 2008, warning of a potential terrorist attack against the Leopold Café in October 2008.²⁸ The notional exercise report stated there was an imminent threat to the U.S., possibly in the Chicago area, from a group of Canadian-Pakistani militants with dual passports working with al-Qaida.

The exercise participants represented fourteen Federal Departments and Agencies, including the FBI, Department of Homeland Security (DHS), Department of Defense (DoD), and the National Security Agency (NSA). Five state and local police departments representing Chicago, New York, Los Angeles, Washington D.C. and Illinois State Police also participated.

The exercise scenario began on a weekend midsummer night when ten al-Qaida operatives notionally entered Chicago after dark via maritime approach on Lake Michigan from Canada. They proceeded to break into two-man teams and near simultaneously, notionally attack eight targets.²⁹

One of the assumptions in the exercise was that the attacks overwhelmed state and local law enforcement agencies and that the Chicago Chief of Police requested federal assistance by

contacting the senior USG law enforcement authority within the city of Chicago: the Special Agent in Charge of the FBI Field Office in Chicago.

Potential Gaps in U.S. Preparedness

During the exercise, two of the same deficiencies discovered in the GoI Mumbai Investigations were also identified by the USG interagency exercise participants:

1. Federal Authority³⁰
2. State and Local Authority³¹

Federal Authority Gap

Indian “paramilitary” forces including the NSG, were severely outmatched in Mumbai, particularly in the area of equipment. This was the case, despite the fact their military and law enforcement agencies are legally authorized to conduct joint operations and training, as well as use the same equipment. The rapid growth of internal GoI intelligence bureaus and the increased use of paramilitary forces against communal unrest have given the Indian Home and Defense Ministries increased control over paramilitary operations. For example, Indian Army units are also deployed for internal security duty.³²

On the other hand, the U.S. Posse Comitatus Act of 1878 does not allow DoD entities to conduct law enforcement operations, without the President and Secretary of Defense’s concurrence and upon the recommendation of the Attorney General. Chapter 263, Section 15 of the Act states: “It shall not be lawful to employ any part of the Army of the United States, as a posse comitatus, or otherwise, for the purpose of executing the laws, except in such cases and under such circumstances as such employment of said force may be expressly authorized by the Constitution or by act of Congress.” Title 10 of United States Code (U.S.C.) Section 375 also incorporates the Air Force, Navy, and Marine Corps within the posse comitatus restrictions.

However, there is one U.S. legal statute, 10 U.S.C. 380, in place to facilitate equipping, training, and information sharing between DoD and state and local law enforcement agencies. But it is irrelevant in today's security environment, when so much emphasis is placed on homeland defense, specifically domestic counterterrorism operations. Besides being outdated, the program itself is underutilized. 10 U.S.C. 380 was signed into law as a result of the FY97 National Defense Authorization Act (NDAA), four years before the tragic events of 9/11.

Section 1033 of FY97 NDAA is tucked in an obscure section within Title X called "General Provisions". General Provisions' main focus is counterdrug, not counterterrorism operations. For instance, the other three sections of Title X all focus on the war on drugs. Section 1031 describes additional support for counterdrug assistance to Mexico. Section 1032 describes availability of funds for certain drug interdiction operations and counterdrug technologies. And Section 1034 focuses on the sale of federal department or agency chemicals used to manufacture controlled substances. Section 1033, created in 1997, does not adequately address post 9/11 state and local law enforcement requirements by federal authorities, including preparations required for a response to a "Mumbai-style" attack in the U.S.

10 U.S. Code § 380 Section 1033³³

When asked, officials from the U.S. Northern Command Judge Advocate General's Office, the National Guard Bureau Contingency Plans Office, and the Office of Secretary of Defense for Homeland Defense (OSD/HD) stated they were unaware of this specific statute. OSD/HD referred me to the Defense Logistics Agency (DLA). DLA representatives said the requirements outlined in 10 U.S.C. 380 are partially performed by the Law Enforcement Support Office (LESO) at DLA.

LESO operates the DoD Surplus Property Program. The office provides briefings on surplus property (requirement (b)(1)(B)) at the annual meeting for the State Points of Contact (appointed by the Governor) co-sponsored by DLA, Department of Justice, and General Services Administration. But, oddly, representatives associated with the Surplus Property Program never heard of the 10 U.S.C. 380 requirements.³⁴ One of the reasons for this is the source references in 10 U.S.C. 380 refer to section 1243 of Public Law 100-180, dated December 4, 1987, prior to the existence of the 1033 Program (Surplus Property Program). Another reason is section 1243 of Public Law 100-180 refers to other reporting requirements that are not the same as the mandate in 10 U.S.C. 380.

Despite this legal dissymmetry, DLA representatives stated they were in partial compliance with 10 U.S.C. 380 through the Defense Reutilization and Management Office (DRMO). DRMO manages the “Section 1033 Program” but not the 1031, 1032, and 1034 programs. DRMO referred me to the “1033 Office”, better known as the LESO, in Battle Creek, Michigan.

The Deputy Director of LESO, Mr. Craig Barrett, said he was also unaware of the 10 U.S.C. 380 statutes but said they were partially complying with Section 1033 Directives. For instance, they sponsor an Annual National Conference (ANC) of State LESO Coordinators. State LESO representatives, usually retired high-ranking law enforcement officers, are responsible for identifying excess military equipment that may be used by their state’s law enforcement agencies. Only one representative from each state attends the ANC, contrary to the 10 U.S.C. 380 stipulation mandating that “law enforcement personnel of the political subdivisions of each state” attend the conference.

According to Barrett, not all states and territories choose to participate in the LESO program. He stated that there are states and territories that are located too far from any military

installations to feasibly take possession of equipment. Some states don't have the funds to resource the acquisition and training of reutilized equipment. But more disturbingly, he said some states are "non-compliant" with DoD regulations.

He also said LESO does not provide any training, expert advice, or other personnel support to state and local law enforcement agencies when distributing reutilized DoD equipment - as stipulated in 10 U.S.C. 380. State and local law enforcement agencies are expected to learn how to use surplus DoD equipment using unclassified manuals on-line or outdated hard-copies of text, even if pieces of surplus military equipment have been discontinued.

Surprisingly, Barrett said that one of the states that doesn't have a relationship with the LESO program is home to the site of the worst terrorist attack in history, New York. Barrett stated that "New York is no longer in compliance with DoD regulations due to corruption charges and equipment misappropriation."³⁵ Barrett stated that New York officials had allegedly reutilized DoD property, then sold it for profit. This is disconcerting when one considers automatic weaponry and up-armored vehicles are available for reutilization and transfer to states.

Despite the legal dissymmetry, when states like New York are non-compliant with a critical equipment reutilization program, there are "whole of government" issues that are systemic even within state and local governments. For example, it appears that there is a disconnect between New York State government and New York City government. Current NYPD Commissioner Raymond Kelly told Congress that New York City was getting cheated out of desperately needed help. Kelly said that the "federal formula is all wrong" for doling out money to counter terror threats.

Kelly asked the Federal Government for \$261 million for city police but received only \$60 million. He complained that almost 80% of the \$3.45 billion in Homeland Security Department

funding for first responders was tied up in formula grants to the states. Only \$800 million was set aside for high-threat urban areas such as New York. He said the formula is "blind to the threats this country faces," and "blind to the consequences of an attack."³⁶ If the NYPD Police Chief needs resources to conduct counterterrorism operations in New York City, then why isn't New York State Government complying with federal regulations and taking advantage of this significantly discounted reutilized equipment?

State and Local Authority Gap

In the ensuing investigations following the Mumbai attacks, the GoI Administrative Reforms Commission recommended the legalized tapping of cellular phones and Internet connections.³⁷ While the GoI considered restricting media coverage of live emergency incidents, broadcasting networks agreed to "self regulate" by implementing delays in live coverage and expunging information about operational details.³⁸ The Indian Constitution, while not mentioning the word "press", provides for "the right to freedom of speech and expression" (Article 19(1) a).

However, this right is subject to restrictions under sub clause (2), whereby this freedom can be restricted for reasons of "sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, preserving decency, preserving morality, in relation to contempt, court, defamation, or incitement to an offense." GoI laws such as the Official Secrets Act and Prevention of Terrorist Activities Act (PoTA) have been used to limit press freedom.³⁹

Internal surveillance on U.S. Persons and forced "self regulation" on media outlets is not in accordance with the First and Fourth Amendments to the U.S. Constitution. But following Mumbai, major U.S. cities, like New York, are examining ways to shut down cell phones when dealing with hostage-taking scenarios. According to NYPD Commissioner Kelly in an open session of the Homeland Security and Governmental Affairs Committee, "Cell phones were

simple tools used to deadly effect in the Mumbai terror attacks. According to phone transcripts, the attackers received instructions and real-time updates about the officers amassing against them. Some of the phones they used for the calls apparently were taken from hostages.”⁴⁰

During the NCTC exercise, the FBI and NSA representatives questioned the New York and Los Angeles police officers after they discussed their respective city’s cell phone monitoring research. The federal participants were concerned that the state and local agencies weren’t sharing their research with the local FBI Field Office Foreign Intelligence Surveillance Act (FISA) agents or Regional Intelligence Center (RIC) officials. The consensus among the state and local officers at the exercise was that they are coordinating and integrating their research with the assistance of federal authorities.

They also agreed that the FISA information sharing process is convoluted, particularly when disseminating federal intelligence reports to state and local agencies. Despite the creation of RICs, DHS, and the Office of the Director of National Intelligence (ODNI), there are still challenges to overcome when sanitizing or producing “tearlined” classified intelligence reports for transfer to state and local agencies before and during attacks. Foreign Intelligence Surveillance Act (FISA).⁴¹

4th Amendment to the U.S. Constitution

“The right of people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated, and no Warrant shall issue, but upon probable cause, supported Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”⁴²

Minimization Procedures

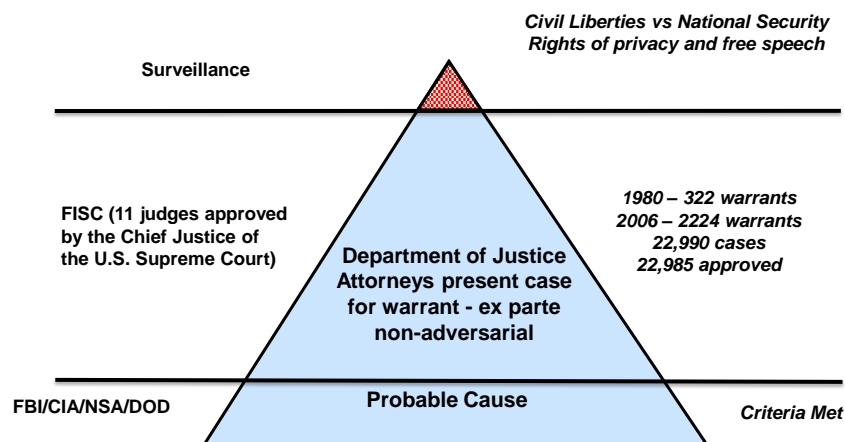


Figure 1. Like any other court of law, agencies applying for a FISA Warrant must meet or exceed the "probable cause" threshold prior to being granted a hearing before the secret Federal Intelligence Surveillance Court. In all likelihood, if this criteria is met, then the warrant will be approved with extremely stringent caveats on surveillance methods and targets.

Federal agencies are working with state and local law enforcement agencies to ensure that their research is within FISA guidelines and that the 4th Amendment is the penultimate consideration in any attempt to obtain a properly administered FISA warrant.

Information Sharing Success Stories

The USG and state and local agencies are collaborating with NCTC to remedy the gaps in the areas of federal, state, and local authorities. There have been recent success stories that suggest information sharing and technology transfer is improving.

For instance, two days before the attacks on the World Trade Center and the Pentagon in 2001, a Maryland State Trooper stopped 9/11 hijacker Ziad Jarrah for speeding near the Delaware state line. The trooper checked Jarrah's license and registration against a database of "wants and warrants," and it came back clean.⁴³ The trooper called the stop routine. He had no way of

knowing that Jarrah was on a CIA watch list and that he was a key player in a major plot to attack the U.S.

If Jarrah was stopped for speeding today, his information would be automatically queried in the FBI's National Crime Information Center (NCIC). His data would be checked against a master list of known or suspected terrorists. The presence of Jarrah's name on this list would raise a flag, and the trooper would be prompted to call the U.S. Terrorist Screening Center (TSC). TSC analysts would run more extensive checks to see if the Jarrah at the traffic stop is the same one of interest to the intelligence community. The screening center would then guide the trooper through some questions for Jarrah or contact an operational unit to coordinate a response, such as an FBI-led Joint Terrorism Task Force.⁴⁴

An example of how this screening process works occurred in Maryland in August 2005. Muhamed Asif Haider, also known as Asif Iqbal, was a passenger in a vehicle that was stopped by Baltimore County Police because the vehicle's lights were not on. The driver could not produce a driver's license so the officer ran a criminal history check on both the driver and passengers. The NCIC database matched Haider to the terrorist watch list. The check showed that Haider fell into a special category that alerted the police officer to potential terrorist involvement. The check also let the officer know that Haider was on the list because he was wanted for questioning in connection with a pending federal indictment in New York. The arresting officer contacted his operations desk, who alerted the local FBI.

The federal indictment said Haider and others sold fraudulent green cards and Social Security cards to an undercover New York police officer and at least one confidential informant. They were suspected of trying to raise money to pay for the illegal travel costs of "additional men" to the United States. While in Baltimore County custody, it was learned that Haider was in the

country illegally, so the FBI and Immigration and Customs Enforcement (ICE) lodged a detainer with authorities in Baltimore County to ensure that he was not released.⁴⁵ Had this routine traffic stop occurred pre-9/11, this stop would most likely have been declared “routine”. Since there were no “wants or warrants” for the driver, the other passenger, or Haider, the police officer would not have known about the ongoing federal investigation, pending indictment, or Haider’s illegal immigrant status.

Conclusion

The international intelligence community warned the GoI twice that Pakistani-trained militants would attack Mumbai up to a year in advance of the attacks.⁴⁶ Even with these advanced warnings, the GoI was unable to deter or counter the Mumbai attacks effectively. How would the U.S. respond if foreign intelligence services shared information pertaining to a pending attack against the homeland?

The provisions for state and local law enforcement agencies to obtain information, equipment, training, expert advice, and other personnel support from DoD are inadequate and need to be modernized and signed into law. This will remove ambiguity and strengthen the “whole of government approach” to homeland security.

The deadly attacks in India may have provided a low-frills but bloody blueprint for other violent groups to follow, NYPD Commissioner Kelly and other U.S. anti-terrorism officials told Congress during a hearing last year. "I think we can expect that groups will look to that (Mumbai) as a model for themselves," Donald Van Duyn, Chief FBI Investigations Officer, said at the hearing.⁴⁷

Last year, General Barry R. McCaffrey, U.S. Army (Ret.), current Adjunct Professor of International Affairs at the United States Military Academy and former Commander, U.S.

Southern Command and former Director, National Drug Control Policy stated: “Terrorists will strike at America during the Obama Administration’s first term.”⁴⁸ Depending on one’s interpretation of the words “terrorists” and “strike”, this prophecy may already have come into fruition considering the attempted “Christmas Day” bombing of a U.S. flagged airliner over Detroit by a self-described member of al Qaida and/or the murders at Ft. Hood by an al Qaida sympathizer.

It is difficult to counter the argument that there are gaps within the USG and state and local law enforcement agencies that require immediate attention if the “whole of government” is going to properly respond to a terrorist attack in the U.S., like the one forecast by Gen. McCaffrey. Rather than criticize, one should look to interagency lessons-learned and success stories to set proper benchmarks for increased cooperation in the future. But, in my opinion, the forecast is calling for rain and the USG’s homeland security apparatus is outside without an umbrella. Denying that there are both gaps in federal statutes and misinterpretations of state and local law enforcement authorities is analogous with the USG laying a counterterrorism foundation that is made of sand.

Bibliography

- ABC News Australia, *"Mumbai Attack Warnings Ignored: A Report,"* Dec 2, 2008.
- Associated Press. *Cops Look to Jam Cell Phones if Terror Strikes.* 2009.
- Barrett, Craig, Deputy Director, Law Enforcement Support Office, Battle Creek Michigan, *Telephone interview*, Oct 13, 2009.
- Bradsher, Keith, and Sengupta, Somini, New York Times, *"India Faces Reckoning as Terror Toll Eclipses 170,"* Nov 29, 2008
- Cable News Network Online. *Tweeting the terror: How social media reacted to Mumbai.* 2008.
- Cable News Network Online. *Botched L.A. Bank Heist Turns into Bloody Shootout.* 1997.
- Congressional Research Office. *Mumbai Attack Summary.* 2008.
- Constitution of the United States of America, *Amendments 1, 4.*
- DHS/TSA Field Intelligence Report (with FBI Sources). *US Files Case Against Mumbai 26 November 2008 Attackers.* 2009.
- Fair, Christine, Dr. RAND Corporation. *The Lessons of Mumbai.* 2009.
- Hindustan Times Online. *Government Decides to Legalize Internet Connections Tapping.* 2008.
- Holcomb, Raymond. National Counterterrorism Center (NCTC). *U.S. Federal Preparedness for Mumbai-Type Attack.* 2009.
- Ignatius, David, Washington Post. *Could Mumbai Happen in the U.S.?* 2008.
- Indian Express Online. *Indian PM Says Mumbai Attack Different from Past Ones, Seeks Political Consensus.* 2008.
- Lapham, Donald, OSD Policy, *Emailed statements to OSD/HD*, Mar 13, 2009.
- Lonely Planet Tour Online Destination Guide. *Mumbai.* 2009.
- Magnier, Mark, Los Angeles Times, *"Systemic Failure Seen in India's Response to Attacks,"* Dec 1, 2008.
- Margolick, David, New York Times. *25 Minutes of Terror in San Francisco.* 1994.
- McCaffrey, Gen (Retired) Barry R., *"Strategic Challenges Facing the Obama Administration,"* Jun 23, 2009.
- Moore, Solomon, Los Angeles Times. *Felons Banned from Sale, Possession of Body Armor.* 1998.
- NCTC Directorate of Strategic Operational Planning, *Mumbai Report*, posted on Intellipedia Page, Sep 22, 2009.
- Prakash, Arun, Adm (Retired). *Mumbai Attack & India's Vulnerable Maritime Flanks.* 2008.
- PTI News Agency. *Indian State Considers Restricting Live Broadcasting During Emergencies – Private Broadcasters to 'Self Regulate' Live Coverage Following Mumbai.* 2008.
- Singh, Madhur, and Thottam, Jyoti, Time Magazine, *"India Faces Questions over Mumbai Siege,"* Nov 29, 2008.
- Sisk, Richard, New York Daily News. *Politicians Fiddle as Kelly Burns Over Anti-terror Funds.* 2003.
- U.S. Daily News, from FBI Sources, *"Look Inside the Terrorist Screening Center,"* Sep 2, 2007.
- Van Duyn, Donald, FBI Chief Investigating Officer, *Statements addressing the Senate Committee on Homeland Security and Government Affairs*, Jan 8, 2009.
- Vernon, August. National Tactical Officers Association. *Mumbai: Vulnerabilities to Soft Target Attacks in U.S. – Project Red.* 2009.
- Washington Post, *Man Arrested in Maryland May Have Terror Ties – On National Watch List,* Aug 10, 2005.

10 U.S.C. § 380. *National Defense Authorization Act (NDAA)*. FY97.

10 U.S.C. § 380, *Enhancement of Cooperation with Civilian Law Enforcement Officials*.

50 U.S.C. Chapter 36, *Foreign Intelligence Surveillance Act*.

50 U.S.C. 1801, 1802, *“Definitions of foreign intelligence information, Foreign Powers, Requirement of the AG to file reports under seal to the FISC,”* Oct 25, 1978.

ENDNOTES

-
- ¹ Government of India (GOI) Press Information Bulletin, “*Statements made by Indian Prime Minister Shri P. Chidambaram*,” Dec 11, 2008
- ² RAND Corp, “*The Lessons of Mumbai Pg. 2*,” Feb 1, 2009
- ³ Lonely Planet Tour Online Destination Guide, “*Mumbai*,” Aug 25, 2009
- ⁴ Adm. Arun Prakash (Ret.) Nov. 30, 2008, *Mumbai Attack & India’s Vulnerable Maritime Flanks*, Dec 1, 2008
- ⁵ Department of State Overseas Security Advisory Council, “*Mumbai Combined Arms Operation*,” Dec 1, 2008
- ⁶ Mumbai Targets:
- Taj Majal Hotel – 105 year old property frequented by celebrities and dignitaries
 - Trident-Oberoi Hotel – formerly Hilton Towers
 - Leopold Café – a popular restaurant and bar frequented by tourists
 - Nariman Jewish Community Center
 - Chhatrapati Shivaji Train Station (Headquarters of Indian Central Railways)
 - Cama & Albles Hospital – a major Mumbai hospital with 367 beds
 - Metro Cinema – a famous Metro-Goldwyn-Mayer (MGM) theater
- ⁷ Navy Department Library, “*Riverine Warfare: The U.S. Navy’s Operations on Inland Waterways*,” Apr 10, 2006
- ⁸ Reuters News International, “*Statements made by India’s Interior Ministry*,” Feb 12, 2009
- ⁹ RAND Corp, “*The Lessons of Mumbai Pg. 5*,” Feb 1, 2009
- ¹⁰ DHS/TSA Field Intelligence Report, “*US Files Case Against Mumbai 26 November 2008 Attackers*,” FBI sources, Aug 21, 2009
- ¹¹ RAND Corp, “*The Lessons of Mumbai Pg. 4*,” 2009
- ¹² Rediff, “*Many More Questions About Terror Attacks*,” Nov 28, 2008
- ¹³ Statements by FBI Chief Investigating Officer Donald Van Duyn while addressing the Senate Committee on Homeland Security and Government Affairs, Jan 8, 2009
- ¹⁴ New York Times, David Margolick, “*25 Minutes of Terror in San Francisco*,” Nov 15, 1994
- ¹⁵ Los Angeles Times, Solomon Moore, “*Felons Banned from Sale, Possession of Body Armor*,” Aug 19, 1998
- ¹⁶ Cable News Network Online, “*Botched L.A. Bank Heist Turns Into Bloody Shootout*,” Feb 28, 1997
- ¹⁷ Washington Post, David Ignatius, “*Could Mumbai Happen in the U.S.*,” Dec 3, 2008
- ¹⁸ Time Magazine, Madhur Singh and Jyoti Thottam, “*India Faces Questions over Mumbai Siege*,” Nov 29, 2008
- ¹⁹ The Times of India Online, “*Mumbai Police Bought Luxury Cars not New Weapons*,” Dec 1, 2008
- ²⁰ Los Angeles Times, Mark Magnier, “*Systemic Failure Seen in India’s Response to Attacks*,” Dec 1, 2008
- ²¹ New York Times, Somini Sengupta and Keith Bradsher, “*India Faces Reckoning as Terror Toll Eclipses 170*,” Nov 29, 2008
- ²² Los Angeles Times, Mark Magnier, “*Systemic Failure Seen in India’s Response to Attacks*,” Dec 1, 2008
- ²³ Los Angeles Times, Mark Magnier, “*Systemic Failure Seen in India’s Response to Attacks*,” Dec 1, 2008
- ²⁴ Wall Street Journal, Geeta Anana, Peter Wonacott, and Matthew Rosenber, “*India Security Faulted as Survivors Tell of Terror*,” Dec 1, 2008
- ²⁵ PTI News Agency, “*India TV Defends Broadcast of Conversations with Mumbai Attackers*,” Nov 29, 2008 available at Open Source Center, SAP2008112950040
- ²⁶ NTOA Project Red Report, “*A Reality Check on the Preparedness of Law Enforcement to Respond to Attacks on Highly Vulnerable U.S. Domestic Targets*,” May 30, 2009
- ²⁷ Report posted on NCTC Directorate of Strategic Operational Planning Intellipedia Page, Sep 22, 2009
- ²⁸ ABC News Australia, “*Mumbai Attack Warnings Ignored: A Report*,” Dec 2, 2008
- ²⁹ Chicago Notional Targets:
- Oak Street Beach (access point)
 - Tavern on Rush (restaurant)
 - Drake Hotel (40 E. Walton Pl)
 - N. Michigan Shops (900 N. Michigan Ave)
 - Four Seasons Hotel (co-located in the same building as N. Michigan Shops)
 - Chicago-Red-Line (“L” Metro stop)
 - Northwestern Memorial Hospital

- Two taxis destroyed by IEDs

³⁰ Federal Gap: The USG lacks the authority under federal law to adequately provide information and training to state and local first responders regarding the availability and sustainability of specialized assets available for reutilization.

³¹ State Gap: Many state and local law enforcement agencies are stretching the boundaries of their constitutional authority when analyzing the conduct of surveillance operations against U.S. persons. This primarily stems from concern over their ability to counter an attack the size and scope of Mumbai.

³² GlobalSecurity.org, "*India Military Guide*," Apr 23, 2009

³³ 10 U.S. Code § 380 Section 1033:

Enhancement of cooperation with civilian law enforcement officials

(a) The Secretary of Defense, in cooperation with the Attorney General, shall conduct an annual briefing of law enforcement personnel of each State (including law enforcement personnel of the political subdivisions of each State) regarding information, training, technical support, and equipment and facilities available to civilian law enforcement personnel from the Department of Defense.

(b) Each briefing conducted under subsection (a) shall include the following:

(1) An explanation of the procedures for civilian law enforcement officials -

(A) to obtain information, equipment, training, expert advice, and other personnel support under this chapter; and
(B) to obtain surplus military equipment.

(2) A description of the types of information, equipment and facilities, and training and advice available to civilian law enforcement officials from the Department of Defense.

(3) A current, comprehensive list of military equipment which is suitable for law enforcement officials from the Department of Defense or available as surplus property from the Administrator of General Services.

(c) The Attorney General and the Administrator of General Services shall -

(1) establish or designate an appropriate office or offices to maintain the list described in subsection (b) (3) and to furnish information to civilian law enforcement officials on the availability of surplus military equipment; and (2) make available to civilian law enforcement personnel nationwide, toll free telephone communication with such office or offices.

³⁴ Emailed statements to OSD/HD from Mr. Donald Lapham, OSD-Policy, Mar 13, 2009

³⁵ Telephone interview with Mr. Craig Barrett, Deputy Director of the Law Enforcement Support Office (LESO), Battle Creek, Michigan, Oct 13, 2009

³⁶ New York Daily News, Richard Sisk, "*Add insult to injury Politicians fiddle as Kelly burns over anti-terror funds*," Oct 22, 2003

³⁷ Hindustan Times Online, "*Government Decides to Legalize Internet Connections Tapping*," Dec 8, 2008

³⁸ PTI News Agency, "*Indian State Considers Restricting Live Broadcasting During Emergencies – Private Broadcasters to ‘Self Regulate’ Live Coverage Following Mumbai*," Dec 3, 2008

³⁹ India Prevention of Terrorism Act, 2002 (Repealed 2006) / GoI Official Secrets Act, 1923

⁴⁰ The Associated Press, "*Cops Look to Jam Cell Phones if Terror Strikes*," Jan 9, 2009

⁴¹ Foreign Intelligence Surveillance Act (FISA): FISA was originally established by the U.S. Congressional Church Committee in 1978. Its main focus was on foreign governments operating within the U.S. It authorized the USG to conduct surveillance for one year without a court order unless a U.S. Person is party. It also created a secret court: The Foreign Intelligence Surveillance Court (FISC) where classified intelligence is not subject to cross-examination and/or public release. The act was originally intended to provide federal authorization to conduct counter-espionage against foreign spies, particularly from former Warsaw Pact countries. Following 9/11, the Patriot Act amended the law to include surveillance against terrorists not backed by foreign governments. As a result the President authorized NSA to intercept communications into and out of the U.S. of persons linked to al-Qaida or other terrorist factions. Little was known about FISA or the existence of the secret FISA Court until the Act came into public prominence in December 2005. A New York Times article described warrantless wiretaps by the USG, especially the NSA, and asserted it was a violation of 4th Amendment rights.

⁴² When state and local law enforcement agencies stated that they were conducting surveillance research, the federal agents were specifically concerned that there may be conflicts in regard to existing and often scrutinized "Minimization Procedures". Minimization procedures are the standards by which federal agents operate to

minimize the intrusion into U.S. Person protections under the 4th Amendment. For instance the FISA Warrant Criteria used by the FBI, NSA, CIA, and DoD are:

- Reasonable procedures in place for determining acquisition connections to persons living outside of U.S. jurisdiction.
- Acquisition does not solely involve domestic communications.
- Acquisition involves obtaining communications from or with assistance of a service provider.
- Significant purpose of acquisition is to obtain foreign intelligence information.
- FISA Minimization procedures will be used

⁴³ U.S. Daily News, from FBI Sources, “*Look Inside the Terrorist Screening Center*,” Sep 2, 2007

⁴⁴ U.S. Daily News, from FBI Sources, *Look Inside the Terrorist Screening Center*,” Sep 2, 2007

⁴⁵ The Washington Post, *Man Arrested in Maryland May Have Terror Ties – On National Watch List*,” Aug 10, 2005

⁴⁶ ABC News Australia, “*Mumbai Attack Warnings Ignored: A Report*,” Dec 2, 2008

⁴⁷ Statements by FBI Chief Investigating Officer Donald Van Duyn and NYPD Commissioner Raymond Kelly while addressing the Senate Committee on Homeland Security and Government Affairs, Jan 8, 2009

⁴⁸ Gen. Barry R. McCaffrey, “*Strategic Challenges Facing the Obama Administration*,” Jun 23, 2009